UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/767,878	01/28/2004	Naoki Asada	60717 (70904)	4109

7590 01/22/2009

Edwards & Angell, LLP
Intellectual Property Practice Group
P.O. Box 55874
Boston, MA 02205

EXAMINER	
GYORFI, THOMAS A	

ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
01/22/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/767,878	ASADA ET AL.	
	Examiner	Art Unit	
	Thomas Gyorfi	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 August 2008 and 27 August 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6 and 8-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6 and 8-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/19/08*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-6 and 8-22 remain for examination. The correspondence filed 8/26/08 and 8/27/08 amended claims 1, 2, 17, and 18.

Response to Arguments

2. Applicant's arguments with respect to claims 1-22 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

4. Claims 1-6, 8-14 and 17-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Burns (U.S. Patent 6,405,315), and further in view of Flyntz (U.S. Patent Application Publication 2002/0147924) in view of "Windows 2000 Quick Fixes" (hereinafter, "Boyce").

Regarding claims 1 and 18:

Burns discloses an electronic device network system comprising: an electronic device for transmitting data via a network (a network client, col. 5, lines 55-60); a plurality of storing means for storing data transmitted from the electronic device (the storage devices, Ibid); a plurality of external devices for acquiring data from the storing means and processing the acquired data (other network clients, Ibid and Figure 1); the

network connecting the storing means, the electronic device, and the external devices to one another (Ibid, and Figs. 1 & 2), wherein the electronic device, at least one of the plurality of storing means, and at least one of the external devices each have a security function (col. 5, lines 25-45), said method searching the plurality of storing means and the plurality of external devices whose respective security functions match a security level set by a user, when the electronic device transmits data (Figure 7) wherein the electronic device transmits the data to one of the given storage means or the given external device responsive to an input from the user selecting the one of the identified given storing means or the identified given external device as the recipient for the transmitted data (col. 9, lines 1-25; col. 13, lines 1-35).

Although Burns disclose a setting section for setting a security level for the data to be transmitted, the set security level being selected by a user from a plurality of identified security levels (col. 9, lines 1-25), it does not appear to disclose wherein the security levels are associated with a device. However, Flyntz discloses wherein individual computers/storage devices can have security levels (paragraphs 0016, 0033, 0034, & 0041; cf. Figures 1 & 2), including a setting section for setting a security level for the data to be transmitted, the set security level being responsive to input from a user of the electronic device and selected from a plurality of identified security levels (Ibid, and paragraphs 0058-0060). It would have been obvious to one of ordinary skill in the art at the time the invention was made to have hardware devices have their own security levels in the invention disclosed by Burns, as all of the claimed elements were known in the art, and one of ordinary skill in the art could have combined the elements

as claimed by known methods, and the result would have yielded predictable results to one of ordinary skill in the art at the time of the invention.

Although neither Burns nor Flint explicitly disclose a selecting means for providing results of the searching to the user and for providing output, the output corresponding to a selected one of the identified one or more given storing means or the identified one or more given external device whose security level corresponds to the security level set in the setting section, the selected one being selected by the user from the provided search results, it is observed that the technique of searching for external storage devices and having a user select one of the results has long since been a feature of operating systems such as Windows 2000; one example of said feature is disclosed by Boyce (section 8.7.1, "Use Search for Computers"). It is further observed that the external devices ("shares": see section 8.11) have at least a rudimentary approximation of security levels (all of section 8.1). Accordingly, it would have been obvious to include a searching means for external storage devices into the invention of Burns in view of Flyntz, as the technique was recognized as part of the ordinary capabilities of one of ordinary skill in the art, given the disclosure of the technique as being a component of prior art operating systems in general.

Regarding claim 17:

Burns discloses a data receiver search system comprising: a plurality of storing means with different security levels for storing data (col. 5, lines 55-60); a plurality of external devices for acquiring data from the storing means and processing the acquired

data (other network clients[1], Ibid); an electronic device connected to the plurality of storing means and the plurality of external devices via a network (the owner's network client, Ibid); and a search device, connected to the electronic device, for searching for a storing means that satisfies predetermined conditions (Figure 7); the electronic device including: a transmission section for transmitting data to the storing means (col. 3, lines 10-25); a setting section for enabling a user to set a security level for transmitted data (Ibid), the search device including a search section for a storing means according to the security level set in the setting section, so that the transmitted data is received by the storing means responsive to an input from the user selecting the identified given storing means as the recipient for the transmitted data (Details on selected File Operation Parameters: col. 12, line 52 – col. 13, line 35).

Although Burns disclose a setting section for setting a security level for the data to be transmitted, the set security level being selected by a user from a plurality of identified security levels (col. 9, lines 1-25), it does not appear to disclose wherein the security levels are associated with the network client devices. However, Flyntz discloses wherein individual computers/storage devices can have security levels (paragraphs 0016, 0033, 0034, & 0041; cf. Figures 1 & 2), including a setting section for setting a security level for the data to be transmitted, the set security level being responsive to input from a user of the electronic device and selected from a plurality of identified security levels (Ibid, and paragraphs 0058-0060). It would have been obvious

[1] Examiner wishes to observe that, unlike in the Miyazaki reference wherein it was assumed that devices inherit the security levels of their user, the newly-discovered Flyntz reference discloses wherein devices have their own security levels, rendering Applicant's arguments vis-à-vis "network clients" moot.

to one of ordinary skill in the art at the time the invention was made to have hardware devices have their own security levels in the invention disclosed by Burns, as all of the claimed elements were known in the art, and one of ordinary skill in the art could have combined the elements as claimed by known methods, and the result would have yielded predictable results to one of ordinary skill in the art at the time of the invention.

Although neither Burns nor Flint explicitly disclose a selecting means for providing results of the searching to the user and for providing output, the output corresponding to a selected one of the identified one or more given storing means or the identified one or more given external device whose security level corresponds to the security level set in the setting section, the selected one being selected by the user from the provided search results, it is observed that the technique of searching for external storage devices and having a user select one of the results has long since been a feature of operating systems such as Windows 2000; one example of said feature is disclosed by Boyce (section 8.7.1, "Use Search for Computers"). It is further observed that the external devices ("shares": see section 8.11) have at least a rudimentary approximation of security levels (all of section 8.1). Accordingly, it would have been obvious to include a searching means for external storage devices into the invention of Burns in view of Flyntz, as the technique was recognized as part of the ordinary capabilities of one of ordinary skill in the art, given the disclosure of the technique as being a component of prior art operating systems in general.

Regarding claim 2:

Burns further discloses wherein the plurality of storing means includes a first storing means having a higher security level, and a second storing means having a lower security level (col. 13, lines 5-15).

Regarding claim 3:

Burns further discloses wherein the first storing means transmits data by encrypting the data (col. 5, lines 25-45), and the second storing means transmits data without encrypting the data (col. 2, lines 4-27).

Regarding claim 5:

Burns discloses wherein each of the storing means can either be on a local area network [i.e. not having access to the Internet] or other network means (col. 5, lines 5-10). Additionally, the prior art technologies that Burns discloses as being analogous to that invention (e.g. NFS, col. 2, lines 5-20) were capable of being connected to the Internet (cf. "more NFS over TCP stuff" reference). Accordingly, it would have been obvious to one of ordinary skill in the art to construe the "other network types" as the Internet itself, as Burns discloses that there existed a need for the ability to share data remotely in an identical manner to how one would access it locally (col. 1, lines 20-30).

Regarding claim 4:

The rationale for rejection of claim 5 also applies to the rejection of claim 4. Furthermore, one of ordinary skill in the art at the time the invention was made would have known to use a firewall to limit access to devices on the Internet, particularly as firewalls are designed to implement access control policy (see page 4 of the previously enclosed "Firewalls FAQ"; cf. Burns, col. 13, lines 5 and 33)

Regarding claim 6:

Burns further discloses wherein the electronic device, at least one of the plurality of storing means, and at least one of the external devices each have a communications function for encrypted data (col. 5, lines 25-45).

Regarding claims 8 and 19:

Burns further discloses search means for searching for an external device according to locations or function of the external devices (Ibid).

Regarding claims 9, 10, and 20:

Burns further discloses wherein the search means searches for a transmission route of the transmitted data from the electronic device to the storing means or external device (Ibid, and also col. 5, lines 25-45).

Regarding claim 11:

Burns further discloses wherein the external devices each include a search section for searching for a storing means whose security level matches a security level of an external device making the search (col. 10, lines 20-50).

Regarding claim 12:

Burns further discloses wherein the electronic device includes a displaying means for displaying a result of search made by a search means according to search conditions (e.g. the "`ls`" command inherent to Unix-based systems: col. 9, lines 20-25).

Regarding claim 13:

Burns further discloses wherein the respective security functions of the electronic device, at least one of the plurality of storing means, and at least one of the plurality of external devices are rendered depending on whether the electronic device, the storing means, and the external devices belong to which of a plurality of networks that are connected to one another via access control means (col. 10, lines 20-50).

Regarding claim 14:

It is taken as Applicant admitted prior art that the computers used in the Burns system would have a monitor or other visual display means, which would make them an "image forming device" under the broadest possible definition in the art.

Regarding claim 21:

Flyntz further discloses prohibiting the transmission of data from the electronic device or from the storing means when the respective associated security levels of the electronic device, the storing means, and the external devices do not match the security level as established by the user (paragraphs 0058-0060) and allowing transmission of data when the electronic device, the storing means, and the external devices do not match the security level as established by the user (Ibid).

Regarding claim 22:

Burns further discloses wherein when stored data in a storing means needs to be outputted from an external device but an external device and a storing means have different associated security levels so that the data is prevented from being transmitted from the storing means to the external device, repeating said step of searching to identify another given external device whose security level matches the security level of the storing means storing the necessary data (col. 10, lines 20-50; col. 13, lines 1-35).

5. Claims 15 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Burns in view of Flyntz in view of Boyce as applied to claims 1 and 14 above, and further in view of Tomat (U.S. Patent 6,459,499).

Regarding claims 15 and 16:

Burns and Flyntz and Boyce disclose or suggest all the limitations of claims 1 and 14 above. Neither Burns nor Flyntz nor Boyce disclose that the electronic device is a scanner; however, Tomat discloses that scanners were capable of transmitting data via a network (col. 2, lines 33-45). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use a scanner as the electronic device to transmit data via a network to the distributed storage of Burns (in view of Flyntz in view of Boyce). The motivation for doing so would be to make it easy for a user to send scanned images to remote systems with a minimum of user intervention (col. 2, 5-25).

Conclusion

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas Gyorfi whose telephone number is (571)272-3849. The examiner can normally be reached on 8:30am - 5:00pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

TAG
12/30/08
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435